

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年12月 9日

出 願 番 号

Application Number:

特願2002-356515

[ ST.10/C ]:

[ JP 2002-356515 ]

出 願 人

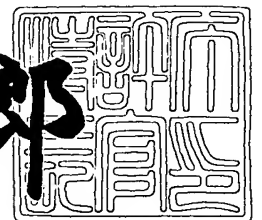
Applicant(s):

コナミ株式会社

2003年 6月25日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3050206

【書類名】 特許願

【整理番号】 P1729

【提出日】 平成14年12月 9日

【あて先】 特許庁長官殿

【国際特許分類】 A63F 13/00  
A63F 13/10

【発明者】

【住所又は居所】 東京都港区芝四丁目 1 番 2 3 号 株式会社コナミコンピ  
ュータエンタテインメントスタジオ内

【氏名】 森 昌二

【特許出願人】

【識別番号】 000105637

【氏名又は名称】 コナミ株式会社

【代理人】

【識別番号】 100107331

【弁理士】

【氏名又は名称】 中村 聡延

【電話番号】 03-5524-2323

【選任した代理人】

【識別番号】 100099645

【弁理士】

【氏名又は名称】 山本 晃司

【電話番号】 03-5524-2323

【選任した代理人】

【識別番号】 100108800

【弁理士】

【氏名又は名称】 星野 哲郎

【電話番号】 03-5524-2323

【先の出願に基づく優先権主張】

【出願番号】 特願2002-272794

【出願日】 平成14年 9月19日

【手数料の表示】

【予納台帳番号】 131957

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0110288

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証処理ハードウェア、認証処理システム、及び、利用管理ハードウェア

【特許請求の範囲】

【請求項 1】 ネットワークを介してサーバ装置と通信可能な端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証処理ハードウェアであって、

前記ユーザの認証情報を記憶する記憶部と、

前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、認証処理のために当該ハードウェアに割り当てられた暗号鍵を受信する暗号鍵受信部と、

受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、

前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、

前記サーバ装置から、暗号化された認証結果情報を受信する認証結果情報受信部と、

前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、

前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備えることを特徴とする認証処理ハードウェア。

【請求項 2】 前記復号化処理部は、1つの前記暗号鍵を利用した復号化処理を1回に限り行うことを特徴とする請求項 1 に記載の認証処理ハードウェア。

【請求項 3】 前記復号化された認証結果情報に基づいて、前記端末装置を制御する制御部をさらに備えることを特徴とする請求項 1 又は 2 に記載の認証処理ハードウェア。

【請求項 4】 ネットワークを介して相互に通信可能なサーバ装置及び端末装置と、前記端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行するハードウェアと、を備える認証処理システムであって、

前記サーバ装置は、

前記ハードウェアからの認証要求に対して、要求元の前記ハードウェアに対して割り当てた暗号鍵を送信する暗号鍵送信部と、

前記ハードウェアから暗号化された認証情報を受信して復号化し、認証結果情報を暗号化して前記ハードウェアに送信する認証結果情報送信部と、を備え、

前記ハードウェアは、

前記ユーザの認証情報を記憶する記憶部と、

前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、前記暗号鍵を受信する暗号鍵受信部と、

受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、

前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、

前記サーバ装置から、暗号化された前記認証結果情報を受信する認証結果情報受信部と、

前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、

前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備え、

前記端末装置は、

前記ハードウェアに対して、前記サーバ装置との間の通信を伴う処理の実行許可を要求する許可要求部と、

前記ハードウェアから前記実行許可を受信したときに前記処理を実行する実行部と、を備えることを特徴とする認証処理システム。

【請求項 5】 端末装置に取り付けられ、前記端末装置の利用可否の管理処理を実行する利用管理ハードウェアであって、

前記端末装置の利用可否を示す利用可否情報を記憶する記憶部と、

前記端末装置から、動作要求を受信する受信部と、

前記利用可否情報に基づいて前記端末装置の利用可否を判定する判定部と、

前記端末装置の利用が可能であると前記判定部が判定したときに、前記端末装置を動作可能とする制御部と、を備えることを特徴とする利用管理ハードウェア

## 【発明の詳細な説明】

## 【0001】

## 【発明の属する技術分野】

本発明は、ネットワークゲームにおけるユーザ認証、利用期間管理などを含むセキュリティ管理手法に関する。

## 【0002】

## 【従来の技術】

近年では、家庭用ゲーム機などの端末装置でインターネットなどを介してゲームサーバに接続することにより、ユーザがネットワークを利用して各種のゲームを楽しむことができるようになっている。このようなゲーム環境は広い意味で「ネットワークゲーム環境」などと呼ばれるが、実際にユーザがネットワークを利用する形態は、幾つかのものがある。

## 【0003】

第1の形態は、ユーザがオンラインでゲームを実行する形態である。即ち、ユーザは、ゲーム機を使用してゲームサーバとの通信を継続した状態でゲーム進行に要するデータをゲームサーバとの間で通信し、ゲームを実行する。この形態では、通常、ユーザがゲームサーバに接続してゲームを開始するたびに、ユーザの認証処理が要求される。つまり、ゲームサーバにアクセスしたユーザが、ユーザ登録などを完了した登録ユーザであるか、又は、実際にゲームサーバにアクセスしているユーザが登録ユーザ本人であるか、などをチェックする。このようなユーザ認証は、一般的にはユーザ登録時に発行されたユーザID及びパスワードをユーザがゲーム機に対して入力し、ゲームサーバへ送信することにより行われる。ゲームサーバは、受信したユーザID及びパスワードが登録ユーザのものであるかをチェックし、ユーザ認証を実行する。

## 【0004】

一方、第2の形態では、ユーザはオンラインでゲームを実行するのではなく、ゲームプログラムの流通手段としてネットワークを利用する。つまり、ユーザはネットワークを介してゲームサーバへ接続し、所望のゲームを選択してそのゲー

ムプログラムを自分のゲーム機へダウンロードする。ダウンロードが完了すればゲームプログラム自体はユーザのゲーム機側に存在するので、原則としてユーザはゲームを実行するためゲームサーバへ接続する必要はなくなる。

## 【 0 0 0 5 】

## 【発明が解決しようとする課題】

ネットワークを利用したゲームにおいては、幾つかの問題がある。その1つはユーザの認証の問題である。上述のように第1の形態においては、ユーザ認証は一般的にユーザIDとパスワードの組み合わせによって行われる。しかし、ユーザIDとパスワードを利用したユーザ認証処理は、以下のような理由でセキュリティ面では非常に弱いと言わざるをえない。

## 【 0 0 0 6 】

まず、ユーザIDやパスワードは第三者による複製、偽造が容易である。ユーザIDやパスワードは単なる文字列であり、しかもユーザがゲーム機に対して手入力することを前提に作成されているため、せいぜい10桁程度の長さであるのが普通である。よって、不正に他の登録ユーザになりすましてゲームを行おうとする者は、何通りもの文字列を推測して入力することにより、比較的容易に他人のユーザIDやパスワードを推測することができる。また、一旦他人に知られると、さらに他の者へと急速に頒布される危険性もある。1つのユーザID及びパスワードを複数人が同時に使用できるので、ユーザIDやパスワードが広まってしまうと、誰もがそれを利用して不正にゲームを行うことができってしまう。

## 【 0 0 0 7 】

ユーザIDやパスワードの桁数を増やせば推測は困難となるのであるが、一般的にユーザIDやパスワードは人間が記憶しておき手入力するものであるから、入力間違いやパスワードの紛失（忘れる）が起きやすい。よって、結局それほど長いユーザIDやパスワードを使用することはできず、安全性の面では自ずと限界がある。

## 【 0 0 0 8 】

さらには、ユーザがゲーム機からゲームサーバへ送信したユーザIDやパスワードを、ネットワーク上の通信途中において傍受して取得したり、ダミーの認証

サーバを構成してゲーム機に対してあたかもユーザ認証が成功したかのように認証結果情報を送信して、不正にゲームを実行可能とすることも可能である。

【0009】

一方、上述の第2の形態のように、ネットワークをゲームプログラムの流通手段として使用する場合には、ユーザに対するゲームの使用期限管理の問題がある。通常、ユーザがダウンロードするゲームプログラムは有料であり、使用料の支払いを条件に一定期間（無期限の場合を含む）ゲームの使用を許可する方式が一般的である。このような場合に、使用期間を管理するために行われる1つの方法は、ユーザがゲームを始める際に、まずゲームサーバへ接続して認証処理を行うことを義務づける方法である。ゲームサーバは、ユーザから接続があると、そのユーザのゲームの使用期限をチェックし、使用期限内である場合にはゲームの実行を許可する情報をゲーム機へ送信してゲームを実行可能とする。

【0010】

しかし、ゲームを開始するたびにゲームサーバへの接続が要求されるというのは、ユーザにとっては煩雑であり、また、通信コストもかかる。よって、使用料の支払いが完了すれば、ユーザにゲームサーバへの接続を行わせることなく、ゲーム機側のみで利用可能な期間を管理することが望まれる。

【0011】

本発明の目的は、以上の点に鑑みてなされたものであり、ネットワークを利用したゲームにおいて、ユーザに煩雑な作業を要求することなく、ユーザの認証や使用期限の管理を確実にを行い、ユーザが安全かつ快適にゲームを行うことを可能とすることにある。

【0012】

【課題を解決するための手段】

本発明の1つの観点では、ネットワークを介してサーバ装置と通信可能な端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証処理ハードウェアは、前記ユーザの認証情報を記憶する記憶部と、前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、認証処理のために当該ハードウェアに割り当てられた暗号鍵を受信する暗号鍵受信部



と、受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、前記サーバ装置から、暗号化された認証結果情報を受信する認証結果情報受信部と、前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備える。

#### 【 0 0 1 3 】

上記のハードウェアは、端末装置に取り付けられることにより、端末装置を使用するユーザの認証処理を実行する。端末装置は、ネットワークを介してサーバ装置と通信可能な装置であり、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などを含む。ハードウェアは、ユーザの認証情報を記憶する記憶部を備える。認証情報は、例えばユーザID、パスワードなどを含むことができる。認証情報は、ハードウェア内部に記憶されており、ハードウェアは内部に記憶した情報に対する外部からのアクセスが不能に構成される。これは、例えば端末装置への取付用コネクタなどの端末装置との入出力手段以外の外部からの入出力手段を設けないなどの方法で実現できる。よって、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。

#### 【 0 0 1 4 】

暗号鍵受信部は、サーバ装置に対して認証処理を要求し、サーバ装置から暗号鍵を受信する。暗号化処理部は、暗号鍵を利用して認証情報を暗号化し、送信部は暗号化された認証情報をサーバ装置へ送信する。認証情報を暗号化して送信することにより、ネットワーク上の送信中に認証情報を取得して複製するなどの不正な使用を防止することができる。サーバ装置は、そうして送信された認証情報に対する認証結果情報を暗号化してハードウェアへ送信する。受信部は、暗号化された認証結果情報を受信し、復号化処理部が暗号鍵を使用して復号化して認証結果情報を取得する。サーバ装置から送信される認証結果情報も暗号化されているので、ネットワーク上で不正に認証結果情報を取得し、悪用することを防止で

きる。その後、認証結果情報の復号化が成功すると、端末装置に実行許可が与えられ、端末装置はサーバ装置との通信を伴う処理の実行が可能となる。

【0015】

なお、暗号化処理部、送信部、受信部及び復号化処理部は、集積回路として構成することができ、これにより各部の内容や機能は外部からは把握不能となり、ハードウェア自体の偽造、複製などを防止することができる。

【0016】

また、記憶部は取り外し可能に構成することができる。これにより、ハードウェアの他の部分を故障その他の理由により交換する必要が生じた場合に、認証情報を記憶した記憶部のみは交換せず、そのまま使用し続けることができる。よって、認証情報を変更する必要なく、ハードウェアの交換やバージョンアップなどに対応することができる。

【0017】

上記の認証処理ハードウェアの一態様では、前記復号化処理部は、1つの前記暗号鍵を利用した復号化処理を1回に限り行う。これにより、サーバ装置から送信された暗号化済みの認証結果情報をネットワーク上で取得し、ダミーの認証サーバなどを利用して端末装置へ送信した場合でも、その暗号化済み認証結果情報に対応する暗号鍵は既に使用済みとなっているため、認証結果情報の復号化は行えない。これにより、ダミーの認証サーバなどを利用した不正な認証処理を防止することができる。

【0018】

上記の認証処理ハードウェアの他の一態様は、前記復号化された認証結果情報に基づいて、前記端末装置を制御する制御部をさらに備える。これにより、認証結果に応じて端末装置を動作させることができる。

【0019】

本発明の他の観点では、ネットワークを介して相互に通信可能なサーバ装置及び端末装置と、前記端末装置に取り付けられ、前記サーバ装置との通信により前記端末装置のユーザの認証処理を実行する認証処理ハードウェアと、を備える認証処理システムが提供される。前記サーバ装置は、前記ハードウェアからの認証

要求に対して、要求元の前記ハードウェアに対して割り当てた暗号鍵を送信する暗号鍵送信部と、前記ハードウェアから暗号化された認証情報を受信して復号化し、認証結果情報を暗号化して前記ハードウェアに送信する認証結果情報送信部と、を備える。また、前記ハードウェアは、前記ユーザの認証情報を記憶する記憶部と、前記サーバ装置に対して認証処理を要求し、前記サーバ装置から、前記暗号鍵を受信する暗号鍵受信部と、受信した前記暗号鍵を利用して前記認証情報を暗号化する暗号化処理部と、前記暗号化された認証情報を前記サーバ装置へ送信する認証情報送信部と、前記サーバ装置から、暗号化された前記認証結果情報を受信する認証結果情報受信部と、前記暗号鍵を利用して、前記暗号化された認証結果情報を復号化する復号化処理部と、前記復号化処理部による前記認証結果情報の復号化が成功した場合に、前記端末装置に、前記サーバ装置との通信を伴う処理の実行許可を与える実行許可部と、を備える。また、前記端末装置は、前記ハードウェアに対して、前記サーバ装置との間の通信を伴う処理の実行許可を要求する許可要求部と、前記ハードウェアから前記実行許可を受信したときに前記処理を実行する実行部と、を備える。

## 【 0 0 2 0 】

上記の認証処理システムによれば、ハードウェアは、端末装置に取り付けられることにより、端末装置を使用するユーザの認証処理を実行する。端末装置は、ネットワークを介してサーバ装置と通信可能な装置であり、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などを含む。ハードウェアは、ユーザの認証情報を記憶する記憶部を備える。認証情報は、例えばユーザID、パスワードなどを含むことができる。認証情報は、ハードウェア内部に記憶されており、ハードウェアは内部に記憶した情報に対する外部からのアクセスが不能に構成される。これは、例えば端末装置への取付用コネクタなどの端末装置との入出力手段以外の外部からの入出力手段を設けないなどの方法で実現できる。よって、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。

## 【 0 0 2 1 】

暗号鍵受信部は、サーバ装置に対して認証処理を要求し、サーバ装置から暗号

鍵を受信する。暗号化処理部は、暗号鍵を利用して認証情報を暗号化し、送信部は暗号化された認証情報をサーバ装置へ送信する。認証情報を暗号化して送信することにより、ネットワーク上の送信中に認証情報を取得して複製するなどの不正な使用を防止することができる。サーバ装置は、そうして送信された認証情報に対する認証結果情報を暗号化してハードウェアへ送信する。受信部は、暗号化された認証結果情報を受信し、復号化処理部が暗号鍵を使用して復号化して認証結果情報を取得する。サーバ装置から送信される認証結果情報も暗号化されているので、ネットワーク上で不正に認証結果情報を取得し、悪用することを防止できる。その後、認証結果情報の復号化が成功すると、端末装置に実行許可が与えられ、端末装置はサーバ装置との通信を伴う処理の実行が可能となる。

## 【 0 0 2 2 】

本発明の他の観点では、端末装置に取り付けられ、前記端末装置の利用可否の管理処理を実行する利用管理ハードウェアは、前記端末装置の利用可否を示す利用可否情報を記憶する記憶部と、前記端末装置から、動作要求を受信する受信部と、前記利用可否情報に基づいて前記端末装置の利用可否を判定する判定部と、前記端末装置の利用が可能であると前記判定部が判定したときに、前記端末装置を動作可能とする制御部と、を備える。

## 【 0 0 2 3 】

上記の利用管理ハードウェアは、端末装置の利用可否の管理を行う。記憶部内には、端末装置の利用可否情報が記憶されている。端末装置から動作要求がなされると、利用管理ハードウェアは利用可否情報に基づいて、端末装置の利用が可能であるか否かを判定する。利用可否情報は、端末装置の使用期限や使用可能日数、使用可能時間数などの時間ベースの情報とすることもできるし、プリペイド式のカウンタ値などのポイント情報とすることもできるし、端末装置を使用するための何らかの特殊な契約や権限に基づく情報とすることもできる。なお、利用可否情報は、これらの例を含めて、端末装置の利用可否の判定に用いることができる各種の情報を含むものとする。例えば、利用可否情報が利用期限の日時や利用可能総時間数などで規定されている場合には、判定部を時計機能により構成することができ、利用可否情報がプリペイド式のカウンタ値などで規定されている

場合には、判定部をカウンタ機能により構成することができる。制御部は、判定部により利用可能と判定された場合に端末装置の動作を許可する。これにより、端末装置の利用可否の管理を容易に行うことができる。

【 0 0 2 4 】

なお、受信部、判定部及び制御部は、集積回路として構成することができる。これにより、各部の内容や機能は外部からは把握不能となり、ハードウェア自体の偽造、複製などを防止することができる

【 0 0 2 5 】

【発明の実施の形態】

以下、図面を参照して本発明の好適な実施の形態について説明する。

【 0 0 2 6 】

〔ネットワークゲーム環境〕

図 1 に本発明を適用したネットワークゲーム環境の概略構成を示す。図 1 において、ゲームの提供者が運営するゲームサーバ 5 と、ユーザが使用するゲーム機 1 6 とがネットワーク 3 を介して通信可能に構成されている。ネットワーク 3 の 1 つの好適な例はインターネットであるが、それ以外のネットワークであってもよい。また、ネットワーク 3 がインターネットである場合には、ユーザのゲーム機 1 6 とネットワーク 3 との間にはインターネットサービスプロバイダ（I S P）その他が介在することとなるが、ここではそれらの説明は省略する。

【 0 0 2 7 】

ゲーム機 1 6 は、好適にはユーザが家庭で使用するゲーム機であるが、遊技場などに設置される業務用のゲーム機であっても構わない。なお、図 1 においては説明の便宜上、1 台のゲーム機 1 6 のみが図示されているが、実際には多数のユーザが所有する多数のゲーム機 1 6 が同様にネットワーク 3 を介してゲームサーバ 5 と通信可能に構成される。

【 0 0 2 8 】

ゲームサーバ 5 は、ユーザに対してネットワーク 3 を通じてゲームを提供する。ゲーム提供の 1 つの形態は、前述のようにゲーム機 1 6 とゲームサーバ 5 との間で通信することにより、ユーザがオンラインでゲームを実行するものである。

この場合、ゲームサーバ5とユーザとが1対1でゲームを実行する場合もあるし、ゲームサーバ5の管理下で複数のユーザが各々ゲーム機16を操作して同時に同一のゲームを実行する場合もある。いずれの場合にも、ユーザは、ゲームを開始するときにゲームサーバ5へ接続し、ユーザ認証処理を行うことになる。

【0029】

一方、前述の第2の形態では、ユーザはネットワークを1つの流通手段として利用し、ゲームサーバ5から所望のゲームプログラムをダウンロードする。ゲームプログラムは通常は有料であり、ユーザはゲームプログラム使用料を、何らかの方法でゲームサーバ5を運営する会社に対して支払う。ゲームプログラム使用料の支払いにより、ユーザは所定期間のゲーム使用权を取得することになる。ゲームサーバ5は、ユーザによるゲームプログラム使用料の支払いを条件に、ネットワーク3を通じてゲームプログラムをユーザのゲーム機16へダウンロードさせる。その後は、ユーザは、既に支払ったゲームプログラム使用权の範囲内（例えば、所定期間内）では、ダウンロードしたゲームプログラムを自由に使用することができる。よって、ゲームサーバ5を運営するゲーム提供者は、使用期限が経過したときにユーザによる当該プログラムの使用を禁止するための方策を採る必要がある。以下、この処理を「使用期限管理」と呼ぶことにする。

【0030】

図1に示すように、本発明のネットワークゲーム環境では、セキュリティモジュール30が使用される。セキュリティモジュール30は、上述のユーザ認証や使用期限管理を行うために使用される専用モジュールであり、ゲーム機16に取り付けて使用される。物理的にはセキュリティモジュール30は内部構造がわからないように製作されたハードウェア装置であり、ゲーム機16の所定のコネクタなどに取り付けられる。ゲーム機16は、セキュリティモジュール30が取り付けられた状態でなければ、ゲームサーバ5を利用したネットワークゲームを実行できないように構成される。なお、ゲームサーバ5とは無関係の市販ゲームソフトなどを使用する場合には、ゲーム機16はセキュリティモジュール30なしでも動作するように構成することができる。本発明では、セキュリティモジュール30を使用することにより、前述のユーザ認証処理や使用期限管理などを、簡

単かつ確実に実行することが可能となる。

【 0 0 3 1 】

[ゲーム機の構成]

次に、図 1 に示すゲーム機の構成について説明する。図 2 はゲーム機 1 6 を含むゲーム装置 2 0 のブロック図である。

【 0 0 3 2 】

このゲーム装置 2 0 は、モニタ 9、スピーカ 1 0 a 及び 1 0 b、コントローラ 1 2、補助記憶装置 1 3、DVD-ROM 1 5、ゲーム機 1 6 で構成される。モニタ 9 には家庭用のテレビ受像機が、スピーカ 1 0 a 及び 1 0 b にはそのテレビ受像機の内蔵スピーカが一般に使用される。スピーカは、右チャンネルスピーカ 1 0 a 及び左チャンネルスピーカ 1 0 b の 2 チャンネルを有する。コントローラ 1 2 は入力装置として機能するものであり、そこにはプレイヤーによる操作を受け付ける操作部材が設けられる。補助記憶装置 1 3 は、ゲーム進行状況などに関連するデータを記憶するための記憶媒体であり、例えば半導体メモリなどを使用することができる。

【 0 0 3 3 】

ゲーム機 1 6 は、マイクロプロセッサを主体として構成された CPU 1 と、その CPU 1 に対する主記憶装置としての ROM 2 及び RAM 3 と、画像処理及び音声処理用のグラフィックスプロセッシングユニット (GPU) 4 及びサウンドプロセッシングユニット (SPU) 6 と、それらのユニットに対するバッファ 5、7 と、DVD-ROM 読取装置 8 と、インターフェース 1 7 と、コネクタ 1 8 と、ハードディスク (HDD) 1 9 と、を有している。

【 0 0 3 4 】

ROM 2 には、ゲーム機の動作制御に必要なプログラムとしてのオペレーティングシステムが格納されている。RAM 3 には記憶媒体としての DVD-ROM 1 5 から読み取ったゲーム用のプログラムやデータが必要に応じて書き込まれる。

【 0 0 3 5 】

GPU 4 は CPU 1 から画像データを受け取ってフレームバッファ 5 上にゲー

ム画面を描画するとともに、その描画された画像のデータを所定のビデオ再生信号に変換して所定のタイミングでモニタ 9 に出力する。SPU 6 は、DVD-ROM 1 5 から読み出されてサウンドバッファ 7 に記録された音声、楽音等のゲーム音データ等を再生してスピーカから出力させる。

【 0 0 3 6 】

DVD-ROM 読取装置 8 は、CPU 1 からの指示に従って DVD-ROM 1 5 上に記録されたプログラムやデータを読み取り、その読み取った内容に対応した信号を出力する。HDD 1 9 には、ゲームサーバ 5 からダウンロードしたゲームプログラムなどが格納される。

【 0 0 3 7 】

コネクタ 1 8 は、セキュリティモジュール 3 0 をゲーム機 1 6 に取り付ける際に使用され、セキュリティモジュール 3 0 側のコネクタと接続される。コネクタ 1 8 は、インターフェース 1 7 を介してバス 1 4 と接続されている。

【 0 0 3 8 】

CPU 1 にはバス 1 4 を介して通信制御デバイス 1 1 が接続され、通信制御デバイス 1 1 にはコントローラ 1 2 及び補助記憶装置 1 3 がそれぞれ着脱自在に接続される。通信制御デバイス 1 1 は一定周期（例えば 1 / 6 0 秒）でコントローラ 1 2 の操作部材の操作状態を走査し、その走査結果に対応した信号を CPU 1 に出力する。CPU 1 はその信号に基づいてコントローラ 1 2 の操作状態を判別する。また、通信制御デバイス 1 1 は、ネットワーク 3 を介してゲームサーバ 5 と必要な通信を行うために機能する。

【 0 0 3 9 】

ゲーム機 1 6 は、記憶媒体としての DVD-ROM 1 5 に記録されたゲームプログラムに従って所定のゲームを実行することができる。また、ネットワーク 3 をゲームプログラムのダウンロード手段として使用する場合には、ゲームサーバ 5 からダウンロードしたゲームプログラムは、ゲーム機 1 6 内部の HDD 1 9 に保存される。よって、ゲーム機 1 6 は、DVD-ROM 1 5 に記録されたゲームプログラムの代わりに、ゲームサーバ 5 からダウンロードし、HDD 1 9 に格納したゲームプログラムに従ってゲームを実行することもできる。



## 【 0 0 4 0 】

ネットワークゲーム実行時には、CPU 1 は、DVD-ROM 1 5 に記録されたゲームプログラム又はゲームサーバ 5 からダウンロードしたゲームプログラムを実行する。そして、その過程で発生する、ゲーム機 1 6 におけるユーザのプレイ状況データを、通信制御デバイス 1 1 及びネットワーク 3 を介してゲームサーバ 5 に送信する。また、必要に応じて、サーバが生成するゲーム状況データや、ネットワーク上で同時にゲームをプレイしている他のユーザのプレイ状況データをゲームサーバ 5 から受信する。こうして、ゲーム機 1 6 はオンラインゲームを進行させる。

## 【 0 0 4 1 】

## 〔セキュリティモジュール〕

次に、セキュリティモジュールについて説明する。図 3 にセキュリティモジュール 3 0 の概略構成を示す。図 3 に示すように、セキュリティモジュール 3 0 は、大別すると、I/F ユニット 3 0 a、処理ユニット 3 0 b 及び記憶ユニット 3 0 c により構成される。セキュリティモジュール 3 0 内部の各ユニットはメモリ、フラッシュ、及び集積回路などを含むハードウェアユニットとして、内部に記憶した情報に対する外部からのアクセスが不能となるように構成される。これは、例えばゲーム機 1 6 への取付用コネクタ 4 0 などのゲーム機 1 6 との入出力手段を除き、外部からの入出力手段や入出力端子を設けないなどの方法で実現できる。

## 【 0 0 4 2 】

I/F ユニット 3 0 は、ゲーム機 1 6 との接続のためのユニットであり、I/F 3 1 と、コネクタ 4 0 とを備える。コネクタ 4 0 は、図 2 に示すゲーム機 1 6 のコネクタ 1 8 と接続される。I/F 3 1 は、セキュリティモジュール 3 0 内のデータとゲーム機 1 6 側のデータとの間のインターフェース処理を行う。

## 【 0 0 4 3 】

記憶ユニット 3 0 c は、認証情報記憶部 3 8 と、不揮発性メモリ 3 9 とを備える。認証情報記憶部 3 8 は、ユーザ ID、パスワードなどの認証情報を記憶する。一方、不揮発性メモリ 3 9 は、認証情報以外の各種情報を記憶する。具体的に

は、ユーザが特定の有料ゲームプログラムをダウンロードした場合の使用期限情報を記憶する。使用期限情報は、例えば「〇年〇月〇日」のように終了日時で記憶してもよく、何百時間というように時間で記憶しても良い。

## 【 0 0 4 4 】

処理ユニット 3 0 b は、CPU などにより構成され、時計機能 3 3、暗号化機能 3 4、復号化機能 3 5 及び通信機能 3 6 を備える。CPU が予め用意された各プログラムを実行することにより、各機能が実現される。時計機能 3 3 は、セキュリティモジュール独自の内部時計であり、基本的に外部からの調整などがないように構成される。

## 【 0 0 4 5 】

暗号化機能 3 4 は、ユーザ認証処理において、認証情報記憶部 3 8 に記憶されている認証情報（ユーザ ID、パスワードなど）を所定の暗号鍵を利用して暗号化する処理を行う。暗号化された認証情報は、ユーザ認証処理においてゲームサーバ 5 へ送られる。復号化機能 3 5 は、ゲームサーバ 5 から送信された暗号化済み情報を復号化する。また、通信機能 3 6 は、暗号化されたユーザ認証情報やゲームサーバから送信される情報などの通信処理を実行する。

## 【 0 0 4 6 】

## [ ユーザ認証処理 ]

次に、ユーザ認証処理について説明する。ユーザ認証処理は、ユーザがゲーム装置 2 0 を使用してゲームサーバ 5 に接続し、ネットワークゲームを開始する際に実行される処理であり、当該ユーザがゲームをプレイすることができる登録ユーザであるか否かを判別するための処理である。

## 【 0 0 4 7 】

通常、ユーザ認証処理においては、ユーザ自身がユーザ ID やパスワードなどの認証情報をゲーム装置 2 0 対して入力し、それがネットワーク 3 を介してゲームサーバ 5 へ送信される。これに対し、本発明では、ユーザ ID 及びパスワードなどの認証情報はセキュリティユニット 3 0 の認証情報記憶部 3 8 内に記憶されており、外部からアクセスすることはできない。即ち、認証情報はハードウェアの形態でセキュリティモジュール 3 0 に実装されているので、複製が困難であり

、また、記憶されている認証情報をセキュリティモジュール 3 0 から外部へ取り出すことも困難である。また、ユーザ自身も、実際に記憶されている認証情報を知らなくても、セキュリティモジュール 3 0 を所持していれば済むので、認証情報自体が漏洩したり、不正に流通することが防止できる。また、万が一第三者が認証情報を知得することができたとしても、その認証情報をユーザ認証処理において入力する術がない。また、セキュリティモジュール 3 0 は物理的な 1 つの存在であるため、複数の人間が同時に使用することはできない。さらに、人間がユーザ ID やパスワードを手入力する場合と異なり、入力ミスも発生しないし、ユーザ ID やパスワードの桁数をかなり長くすることができるので安全性をより高めることができる。

## 【 0 0 4 8 】

次に、セキュリティモジュール 3 0 とゲームサーバ 5 との間で行われるユーザ認証処理について説明する。なお、セキュリティモジュール 3 0 から入出力されるデータは、まずゲーム機 1 6 に入力されることになるが、ゲーム機 1 6 内を単に通過するだけであり、ゲーム機 1 6 はそのデータに対して特に処理を行わない。つまり、ユーザ認証処理は実質的にセキュリティモジュール 3 0 とゲームサーバ 5 との間で実行されることになる。

## 【 0 0 4 9 】

ユーザ認証処理においては、セキュリティモジュール 3 0 内に記憶されているユーザの認証情報（ユーザ ID、パスワードなど）を、ネットワーク 3 を介してゲームサーバ 5 へ正しく送信することが要求される。また、その際に、第三者が送信されたデータをネットワーク上で不正に傍受し、認証情報を知得することを防止しなければならない。このため、本実施形態では、セキュリティモジュール 3 0 は、暗号化機能 3 4 により認証情報を暗号化してからゲームサーバ 5 へ送出する。これにより、第三者がネットワーク 3 上で送信されたデータを取得し、それから認証情報を解析することが防止できる。

## 【 0 0 5 0 】

また、ゲームサーバ 5 上で登録ユーザに対するユーザ認証が正しく完了すると、ゲームサーバ 5 はその旨の通知、つまり、当該ユーザのゲーム機 1 6 にゲーム

の実行を許可するための許可情報をセキュリティモジュール30へ送信することになる。セキュリティモジュール30は、この許可情報を受け取ると、ゲーム機16を制御してゲームの実行を可能とする。ゲームサーバ5はこの許可情報も暗号化して送出する。

## 【0051】

一方、ユーザのゲーム使用期間が終了した場合、当該ユーザは同様の手順でゲームサーバ5へユーザ認証を行っても、ゲームサーバ5側は当該ユーザのゲーム使用期間が終了したことを知っているので、ユーザ認証は不成功に終わる。

## 【0052】

そのような場合、当該ユーザは、ゲーム使用期間満了前に正しくユーザ認証処理が行われた際にゲームサーバ5からセキュリティモジュール30へ送信された許可情報をネットワーク3上で取得しておき、ゲーム使用期間の終了後にダミーサーバ（偽りのゲームサーバとして機能する）を用意して、同じ許可情報をダミーサーバから自己のゲーム機16へ送信しようとすることがありうる。こうすると、ゲーム機16は、ダミーサーバからの許可情報をゲームサーバ5からの許可情報であると誤認し、ゲームを実行してしまう可能性がある。

## 【0053】

このような不正なユーザ認証を防止するために、本実施形態では、ゲームサーバ5からセキュリティモジュール30へ送信される許可情報（暗号化済み）を1回限り有効とする。即ち、1つの許可情報は、セキュリティモジュール30上において一回のみ有効であるとする。これは、例えばセキュリティモジュール30内に、過去にゲームサーバ5から受信した許可情報の履歴を保存しておき、過去に使用された許可情報と同一の許可情報を再度受け取っても、その許可情報を無効とし、ゲームの実行を許可しないようにすることにより実現することができる。

## 【0054】

また、許可情報を1回限り有効とする代わりに、許可情報を暗号化する鍵を1回限り有効とする方法もある。即ち、ゲームサーバ5は、特定の暗号鍵を使用して許可情報を暗号化し、セキュリティモジュール30へ送信する。セキュリティ

モジュール 30 は、その暗号鍵をゲームサーバ 5 から取得しており、当該暗号鍵を使用して許可情報を復号化し、ゲームを実行可能とする。ここで、セキュリティモジュール 30 内では、一度使用された暗号鍵はその後の許可情報の復号化処理には使用できないように構成しておく。こうすれば、前述のダミーサーバから過去に使用した暗号鍵で暗号化された許可情報をゲーム機 16 に再度送って不正にゲームを実行しようとした場合でも、その暗号鍵は既に過去に使用履歴があり、再度使用することはできないので、セキュリティモジュール 30 は許可情報を得ることができない。これにより、使用期間経過後などの不正なゲーム実行を防止することができる。

## 【 0 0 5 5 】

次に、ユーザ認証処理の具体例について図 4 を参照して説明する。図 4 は、ユーザ認証処理のフローチャートである。まず、セキュリティモジュール 30 は、ゲームサーバ 5 へ接続し、ユーザ認証を行う旨を要求する（ステップ S1）。ゲームサーバ 5 は、これに対して、所定の暗号鍵を作成し、セキュリティモジュール 30 へ送信する（ステップ S2）。なお、暗号鍵は、セキュリティモジュール 30 とゲームサーバ 5 との間で認証情報や許可情報を送受信する際の暗号化及び復号化に使用される鍵であり、例えば乱数などとすることもできる。

## 【 0 0 5 6 】

セキュリティモジュール 30 は、暗号鍵を受信すると、認証情報記憶部 38 から認証情報を取得し、これを暗号鍵で暗号化することにより暗号化した認証情報を作成してゲームサーバ 5 へ送信する（ステップ S3）。認証情報は、例えばユーザ ID、パスワードなどを含む。ゲームサーバ 5 は、暗号化した認証情報を受信し、暗号鍵を使用して復号化することにより、認証情報を取得する（ステップ S4）。そして、ゲームサーバ 5 は、認証情報が登録ユーザのものであるか否かを判定する（ステップ S5）。これは、例えば登録ユーザについてのユーザ情報を記憶したデータベースなどを参照して、受信した認証情報が正規な登録ユーザのものであるか否かを判定することにより行われる。

## 【 0 0 5 7 】

認証情報が正規な登録ユーザのものであった場合（ステップ S5 ; Yes）、ゲ

ームサーバ5はゲーム実行許可情報を生成し、これを暗号鍵で暗号化して暗号化済み許可情報を作成する（ステップS6）。一方、認証情報が正規な登録ユーザのものでなかった場合（ステップS5：No）、ゲームサーバ5は所定のエラー処理を行い、ダミーデータを作成する（ステップS7）。ここで、ダミーデータは、不正な目的によりデータの解析が行われることを防止するために生成されるものであり、例えば全く無意味なデータとすることができる。そして、ゲームサーバ5は、ステップS6で生成された暗号化済み許可情報又はステップS7で生成されたダミーデータを、認証結果情報としてセキュリティモジュール30へ送信する（ステップS8）。

## 【0058】

セキュリティモジュール30は、認証結果情報を受信すると、暗号鍵でこれを復号化し（ステップS9）、ゲーム実行が許可されたか否かを判定する（ステップS10）。認証結果情報が暗号化済み許可情報である場合、ステップS9の復号化処理により、暗号化が解除された許可情報が得られる。よって、セキュリティモジュール30は、ゲーム装置20に対してゲーム実行を許可し、ゲームを実行させる（ステップS11）。一方、認証結果情報がダミーデータである場合、ステップS9の復号化は正しく行うことができないので、セキュリティモジュール30はゲームの実行が許可されていないと判断し、ゲーム装置20に対してゲームの実行許可を与えない（ステップS12）。

## 【0059】

以上のようにして、暗号鍵を使用して暗号化した認証情報及び許可情報を通信することにより、ユーザ認証がなされる。ゲームサーバ5は、セキュリティモジュール30からユーザ認証の要求を受けるたびに、新しい暗号鍵を作成し、セキュリティモジュール30へ送信する。従って、ステップS6で生成される許可情報は必ず新しい暗号鍵により暗号化されていることになり、セキュリティモジュール30は新しい暗号鍵を有する正当な登録ユーザでなければゲーム実行を可能とする許可情報を取得することができない。

## 【0060】

また、セキュリティモジュール30は、一度ゲームサーバから受信した暗号鍵

を 1 回限り使用し、繰り返し使用しないこととする。これは、例えば、ユーザ認証要求を行うたびに、その後のステップ S 3 でゲームサーバ 5 から受信した暗号鍵のみを使用するようにプログラムを構成するとか、一度ステップ S 9 の復号化処理で使用した暗号鍵を消去するなど、いくつかの方法で実現することができる。

#### 【 0 0 6 1 】

この方法によれば、前述のダミーサーバを利用した不正な認証処理も不成功とさせることができる。例えばあるユーザがプログラム使用期限の終了などにより正当にゲームを実行できなくなった状態で、前述のダミーサーバを用意し、過去にゲームサーバ 5 から送信された認証結果情報を偽りの認証結果情報としてダミーサーバからセキュリティモジュール 3 0 に送信したとする。セキュリティモジュール 3 0 はステップ S 9 で認証結果情報を復号化するが、その認証結果情報を正しく復号化できる暗号鍵は過去に既に使用済みであり、セキュリティモジュール 3 0 はその暗号鍵を 1 回のみ使用することとしているので、当該偽りの認証結果情報に基づいてセキュリティモジュール 3 0 がゲーム実行許可を発することはない。よって、ダミーサーバを利用する不正な認証処理を無力化することができる。

#### 【 0 0 6 2 】

なお、暗号化処理は一般的には特定の関数による演算処理であり、暗号鍵は当該関数の演算処理に使用するパラメータを示すデータとすることができる。

#### 【 0 0 6 3 】

##### [使用期限管理]

次に、使用期限管理について説明する。使用期限管理とは、事前にゲーム使用料を支払ってゲームの使用権を得たユーザに対して、使用期限を管理し、使用期間経過後はゲームの使用を禁止するための処理である。このような使用期限管理は、ゲーム使用権を得た後でも、ユーザに対して常にゲーム開始前にゲームサーバ 5 へ接続してユーザ認証を行うことを義務付ければ、ゲームサーバ側で容易に行うことができる。しかし、正当な使用期間内であるにも拘わらず、ゲーム開始時にいちいちゲームサーバへ接続して認証処理を行うことは、ユーザにとっては

煩雑であったり、不快であったりする。また、ゲームサーバへ接続することにより、通信コストが発生し、ユーザはこれを負担する必要がある。よって、一度ゲームプログラム使用料を支払った後は、ゲームサーバへ接続する必要なく、ゲーム機側のみで使用期限の管理ができることが望ましい。本発明では、セキュリティモジュール 3 0 によりこれを実現する。

## 【 0 0 6 4 】

具体的には、図 3 に示すセキュリティモジュール 3 0 の不揮発性メモリ 3 9 内に、使用期限情報が格納される。使用期限情報は、例えば何年何月何日まで使用可能であるという日時の情報、又は、合計何時間使用可能であるなどの時間情報などの形態で記憶することができる。

## 【 0 0 6 5 】

また、セキュリティモジュール 3 0 内部の時計機能 3 3 は、基本的に外部からの調整ができないように構成される。よって、ユーザがセキュリティモジュール 3 0 内の時計機能 3 3 にアクセスし、時刻を調整、変更することはできない。通常、ゲーム機 1 6 内にも時計機能は内蔵されているが、これはユーザにより容易に変更可能に構成されている。よって、ゲーム機 1 6 内の時計機能を利用して使用期限を管理するのでは、ユーザによる不正な時刻変更が容易に行われてしまう。この点、本発明のセキュリティモジュール 3 0 によれば、内部の時計機能 3 3 は外部からは変更不能であるので、使用期限を正しく管理することができる。

## 【 0 0 6 6 】

使用期限管理処理の一例を図 5 を参照して説明する。図 5 は、使用期限管理処理のフローチャートである。まず、ユーザが特定のゲームを実行すべくゲーム機 1 6 を操作すると、ゲーム機 1 6 はセキュリティモジュール 3 0 に対してゲーム実行要求を行う（ステップ S 3 0）。セキュリティモジュール 3 0 は、ゲーム実行要求を受け取ると、まず不揮発性メモリ 3 9 から使用期限情報を取得し（ステップ S 3 1）、次に時計機能 3 3 を利用して使用期限内であるか否かを判定する（ステップ S 3 2）。

## 【 0 0 6 7 】

使用期限を過ぎている場合（ステップ S 3 3 ; No）、セキュリティモジュール



30はゲーム機に対してゲーム実行を許可しない（ステップS34）。一方、使用期限内である場合（ステップS33；Yes）、セキュリティモジュール30はゲーム機に対してゲーム実行許可を与える。よって、ユーザはゲームを実行することができる。

#### 【0068】

なお、上記の説明では使用期限管理を日時や時間情報により行う例を示したが、本発明における使用期限管理はそのような時間による管理には限定されない。例えば、使用期限をゲーム何回分などという使用回数として設定し、セキュリティモジュール30内にカウンタ機能を設けて使用回数をカウントすることにより使用期限を管理することもできる。また、ユーザが複数のゲームを選択的にプレイできる環境では、使用可能なポイント数を予めセキュリティモジュール30内に記憶し、ユーザがあるゲームをプレイすると、そのゲームに対応するポイント数だけセキュリティモジュール30内に記憶されたポイント数を減算していくこともできる。この場合のポイント数は、ゲームをプレイするためのプリペイド方式の電子マネー的な意味を有することになる。なお、そのようにセキュリティモジュール内にカウンタ機能を設ける場合には、前述の時計機能と同様に外部からカウント値の調整やリセットなどが不能なようにカウンタ機能を構成する。

#### 【0069】

##### 〔変形例〕

上記の実施例においては、セキュリティモジュール30をゲーム機16に取り付け、セキュリティモジュール30とゲームサーバ5との間のデータ通信はゲーム機16内を通過するように構成されていた。代わりに、図6に示すように、セキュリティモジュール30がネットワーク3に接続され、ゲーム機16へはセキュリティモジュール30内を通過してデータが供給されるように構成することもできる。この場合、セキュリティモジュール30によるユーザ認証の対象となるデータはセキュリティモジュール30による処理後にゲーム機16に送られる。一方、セキュリティモジュール30の処理対象外のデータ（例えば無償のゲームプログラムのダウンロードなど）は、セキュリティモジュール30内をそのまま通過してゲーム機16へ送られる。

## 【 0 0 7 0 】

図 3 に示すように、セキュリティモジュール 3 0 は I / F ユニット 3 0 a、処理ユニット 3 0 b 及び記憶ユニット 3 0 c により構成されている。ここで、セキュリティモジュール 3 0 は、3 つのユニットを一体的に構成することもできるが、記憶ユニット 3 0 c のみを例えばカード型の記憶媒体などとして、他の 2 つのユニットから取り外し可能に構成することもできる。これには以下のようなメリットがある。3 つのユニットが一体的に構成されていると、例えば I / F ユニット 3 0 a 及び処理ユニット 3 0 b 内のいずれかの箇所が故障したような場合、3 つのユニット全体として交換を行う必要がある。また、故障に限らず、セキュリティモジュール 3 0 による処理が多機能化したような場合にも、セキュリティモジュール全体を交換する必要があるが生じる。しかし、記憶ユニット 3 0 c はユーザの認証情報及びゲームの使用期限情報などの情報を記憶したユニットであるので、これを含めてセキュリティモジュール 3 0 全体を交換してしまうと、記憶ユニット 3 0 c 内に記憶されている認証情報やゲーム使用期限情報などを使用不可となってしまう。この点、記憶ユニット 3 0 c のみを取り外し可能に構成しておけば、上記のような理由で他の 2 つのユニットを交換する必要が生じた場合でも、記憶ユニット 3 0 c 内の認証情報などをそのまま引き継ぐことができる。

## 【 0 0 7 1 】

## 【発明の効果】

以上説明したように、本発明によれば、ネットワークを利用したゲームにおいて、ユーザに煩雑な作業を要求することなく、高いセキュリティを確保してユーザが安全かつ快適にゲームを行うことが可能となる。

## 【図面の簡単な説明】

## 【図 1】

本発明を適用したネットワークゲーム環境の概略構成を示すブロック図である。

## 【図 2】

ゲーム装置の概略構成を示すブロック図である。

## 【図 3】

セキュリティモジュールの内部構成を示す機能ブロック図である。

【図 4】

ユーザ認証処理のフローチャートである。

【図 5】

使用期限管理処理のフローチャートである。

【図 6】

本発明の変形例によるゲーム機とセキュリティモジュールの構成を示すブロック図である。

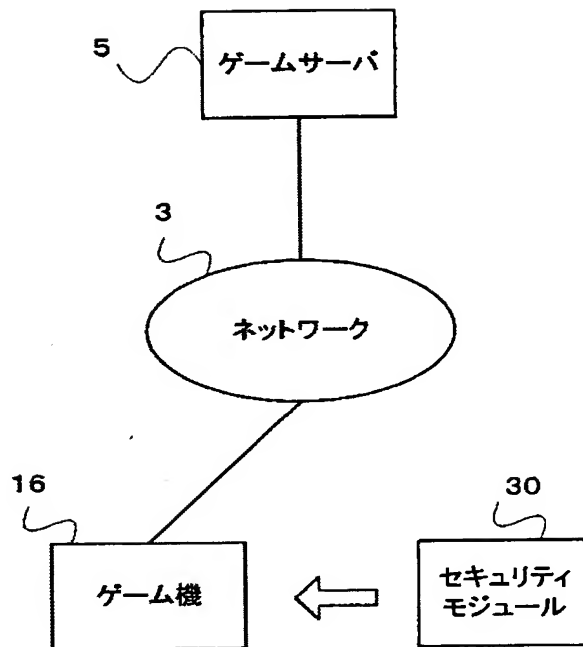
【符号の説明】

- |     |                    |
|-----|--------------------|
| 1   | C P U              |
| 2   | R O M              |
| 3   | R A M              |
| 4   | G P U              |
| 5   | フレームバッファ           |
| 6   | S P U              |
| 7   | サウンドバッファ           |
| 8   | D V D - R O M 読取装置 |
| 9   | モニタ                |
| 1 1 | 通信制御デバイス           |
| 1 2 | コントローラ             |
| 1 3 | 補助記憶装置             |
| 1 4 | バス                 |
| 1 5 | D V D - R O M      |
| 1 6 | ゲーム機               |
| 2 0 | ゲーム装置              |
| 3 0 | セキュリティモジュール        |

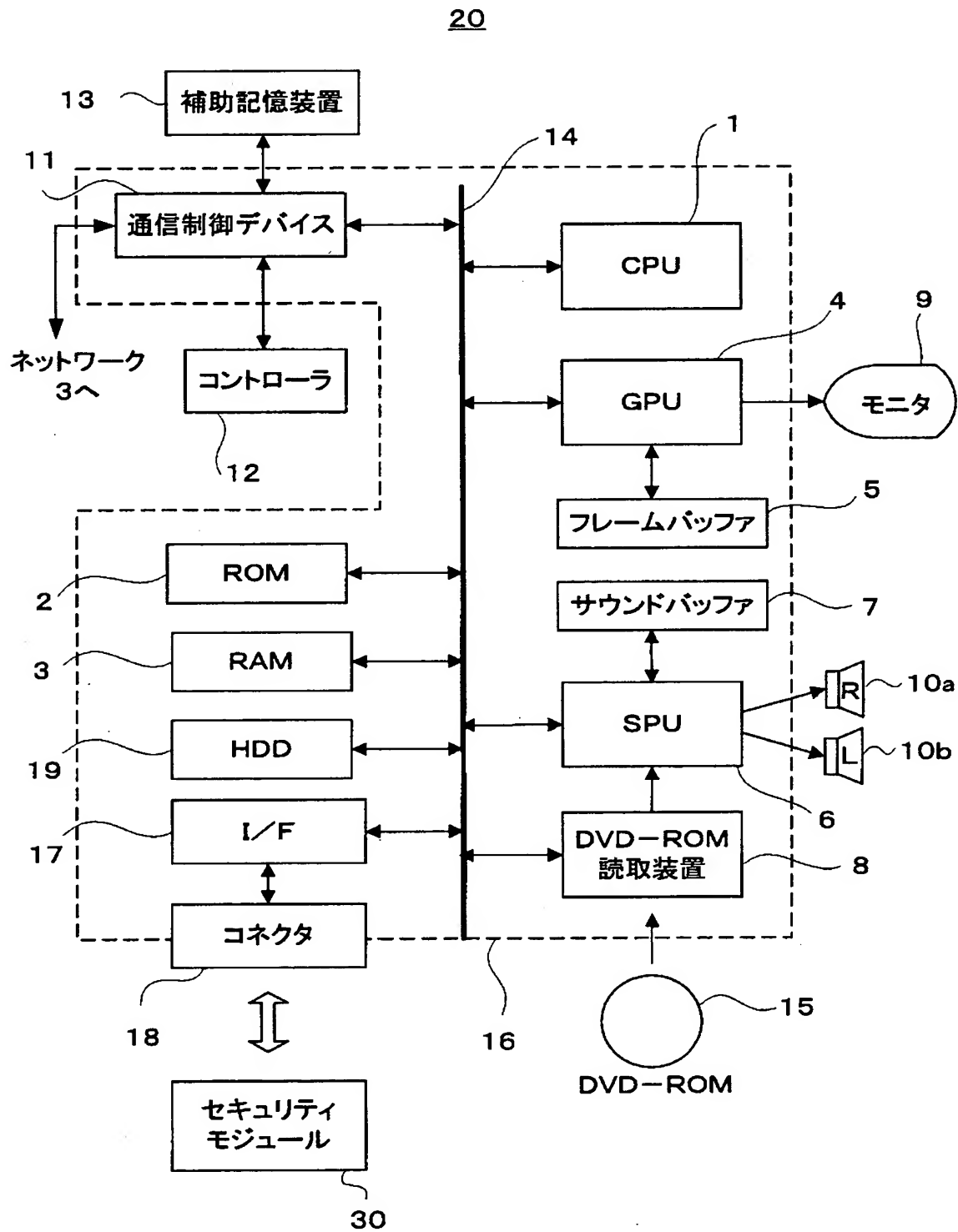
【書類名】

図面

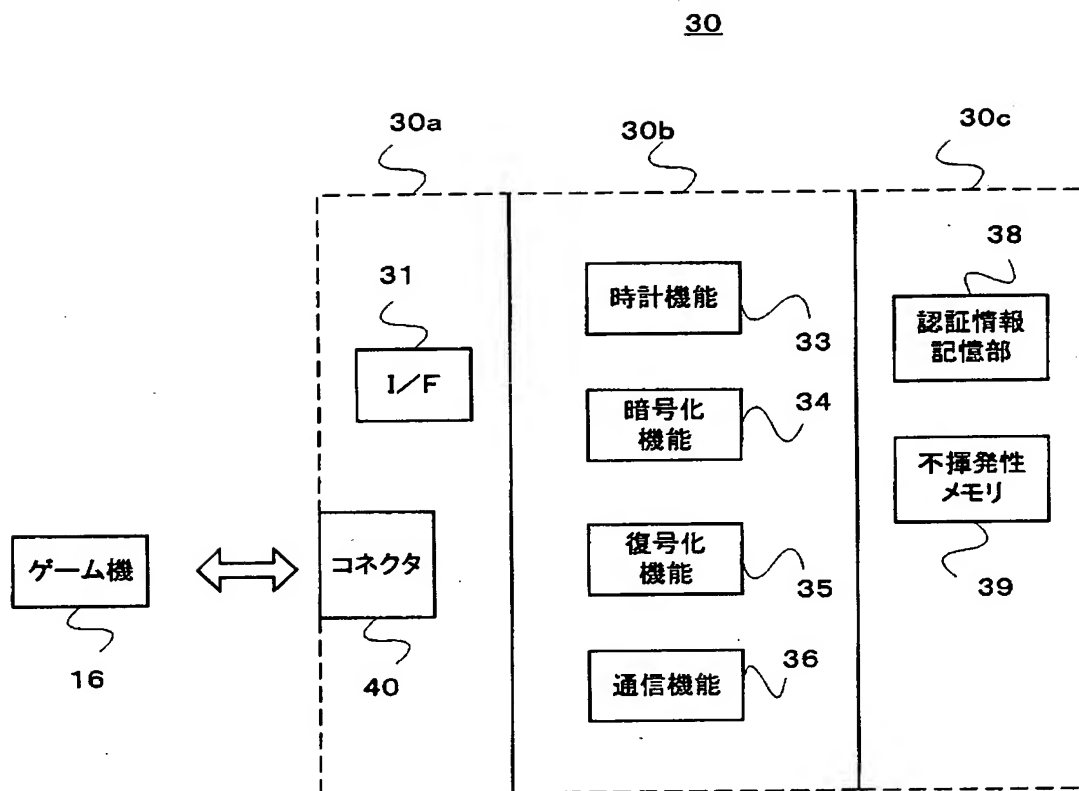
【図 1】



【図 2】



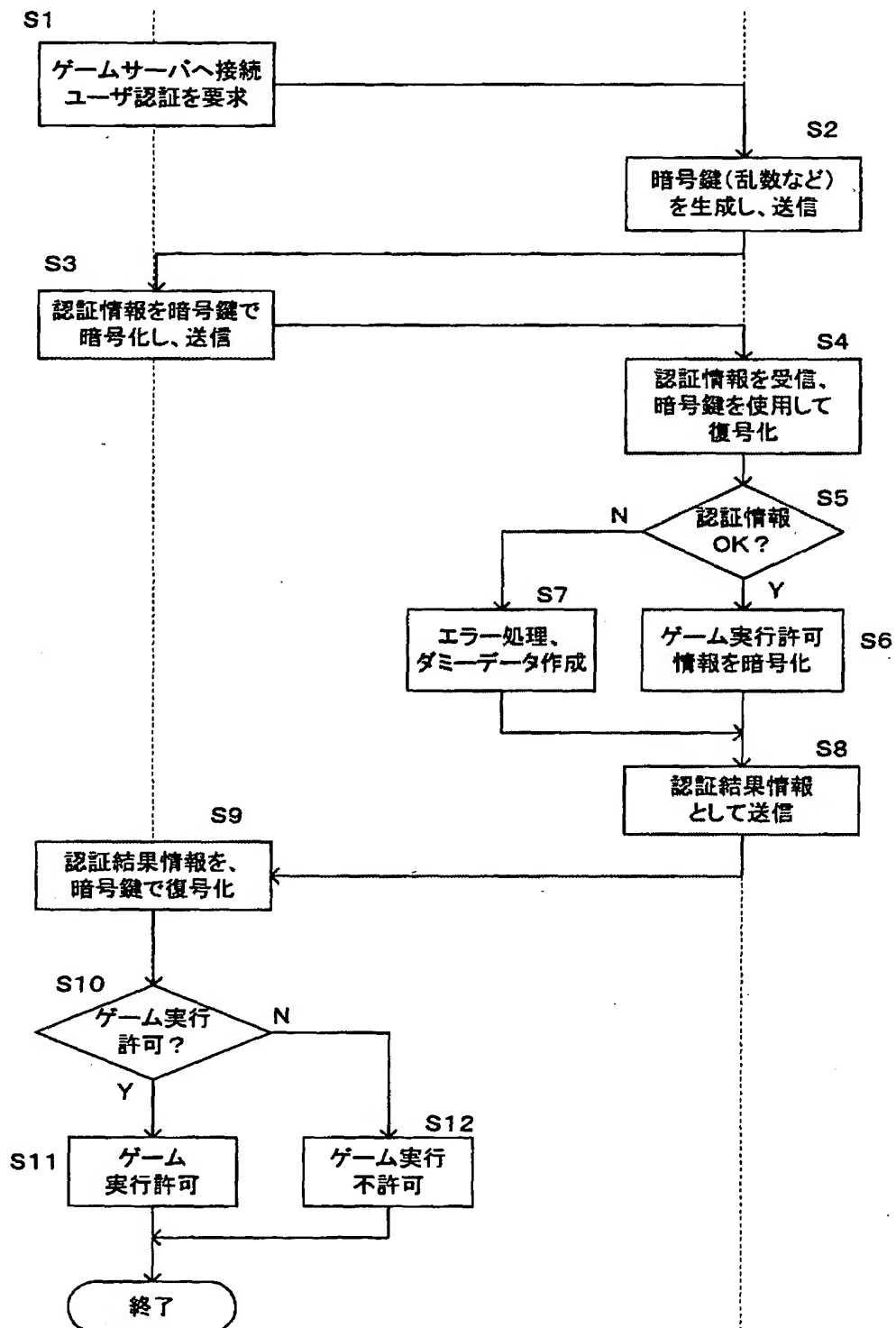
【図 3】



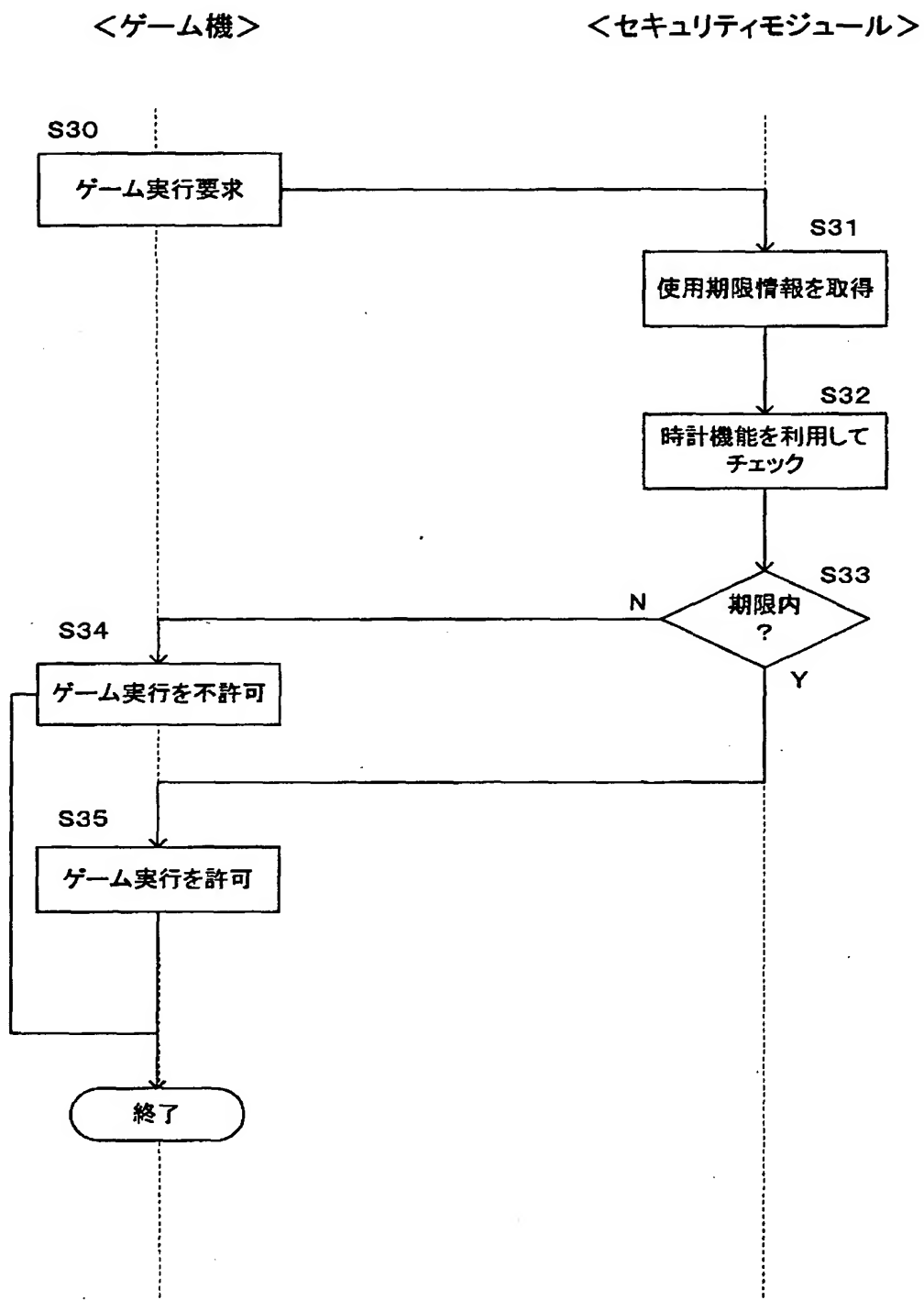
【図 4】

<セキュリティモジュール>

<ゲームサーバ>

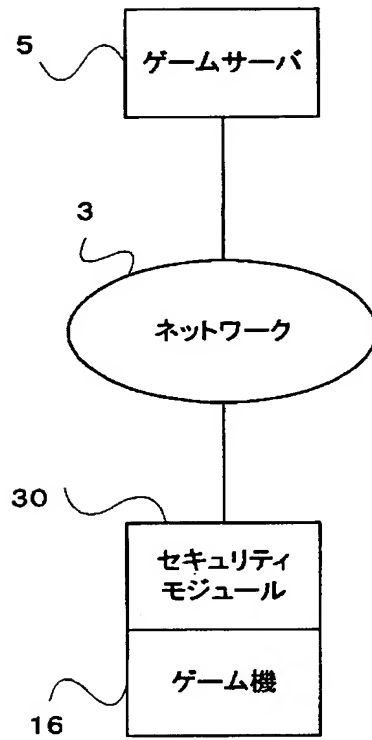


【図 5】





【図 6】



【書類名】 要約書

【要約】

【課題】 ネットワークを利用したゲームにおいて、ユーザに煩雑な作業を要求することなく、高いセキュリティを確保してユーザが安全かつ快適にゲームを行うことを可能とする認証処理ハードウェア及びシステムを提供する。

【解決手段】 認証処理ハードウェアは、ネットワークゲーム環境においてゲームサーバと接続するために使用されるゲーム機などに取り付けられ、ユーザの認証処理を実行する。認証処理ハードウェアは、ユーザの認証情報を記憶する記憶部と、サーバ装置から与えられた暗号鍵で認証情報を暗号化してサーバ装置へ送信する認証情報送信部と、サーバ装置から認証結果情報を受信する認証結果情報受信部と、認証結果情報を復号化する認証結果復号化处理部とを備える。認証情報は、例えばユーザID、パスワードなどを含むことができる。認証情報は、認証処理ハードウェア内部に記憶されており、ハードウェアの外部からはその内容を参照したり、複製したりすることができないので、認証情報の秘密性を確保することができる。よって、ユーザがユーザIDやパスワードを手入力するユーザ認証方法と比べて、安全性を大幅に改善することができる。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000105637]

1. 変更年月日	2002年 8月26日
[変更理由]	住所変更
住 所	東京都千代田区丸の内2丁目4番1号
氏 名	コナミ株式会社